Maine State Government
Dept. of Administrative & Financial Services
Office of Information Technology (OIT)

Major Incident Procedure

1.0 Purpose

This procedure sets OIT's *Major Incident* command, control, and communication protocol. Utilizing a pre-defined procedure, agencies and OIT will collectively ensure the best possible response to Major Incidents.

2.0 Definitions

2.1 **Disaster**: A subset of Major Incidents; those with a *catastrophic* impact. Examples include:

- OIT data center fire, disabling the majority of information operations.
- Cyber-attack that shuts down the entire State network.
- OIT Office building fire or destruction.
- Terrorist attack or accidental destruction of critical IT infrastructure.

2.2 **Major Incident:** Event judged to have a *significant* impact on governmental information operations. Examples include:

- Network, email, or other application outage (possibly including agency applications), for two hours or longer, significantly affecting governmental productivity and/or public service.
- Security breach, significantly compromising either the credibility or operational capability of the government.
- Any event that requires temporary relocation of OIT employees to alternate work sites.

2.3 **OIT Emergency Operations Center:** Default command and control location (51 Commerce Drive, Room 412).

3.0 Applicability

This procedure applies to:

3.1 Executive-branch agencies, irrespective of where their applications are hosted.

3.2 Other State government branch applications hosted by OIT and/or utilizing the State WAN.

3.3 Information Technology (I.T.) Major Incidents exclusively and does not apply to non-I.T. Major Incidents.

4.0 Responsibilities

4.1 Account Managers - (AMs): Communicates or acts as a liaison to key agency personnel during the Major Incident. Disseminates official communication received from the Communications Coordinator.

4.2 Chief Information Officer (CIO): Owns, executes, and enforces this procedure, communicates to Commissioners, determines and declares a *Disaster.*

4.3 Chief Information Security Officer (or designee): Serves as Incident Response Team Leader for cybersecurity incidents. Has authority to declare a Major Incident for any imminent cybersecurity threat.

4.4 Communications Coordinator: Coordinates all internal and external Major Incident communication. Works closely with the AMs to keep all parties informed. Provides accurate and timely updates to the Customer Support Status (CSS) page.

4.5 Duty Manager: Facilitates initial remediation for any incidents and I.T. outages during offbusiness hours and reports potential Major Incidents to the Chief Information Security Officer and Senior Leadership Team members, as appropriate.

4.6 Incident Response Team: Responds to a Major Incident.

4.7 Incident Response Team Leader: Manager/Director closest to the situation. Owns, manages, and leads Major Incident response. Forms and manages the Incident Response Team, serves as, or designates, the Communications Coordinator.

4.8 OIT Senior Leadership Team (members or designees): Determines and declares a Major Incident.

5.0 Directives

5.1 Awareness & Initiation

5.1.1 Any non-OIT Employee suspecting a *potential* Major Incident immediately notifies OIT Customer Support (624-7700).

5.1.2 Any OIT Employee that becomes aware of a *potential* Major Incident immediately notifies their manager/director.

5.1.2.1 The manager/director reports any potential cybersecurity incident to both the Chief Information Security Officer (or designee) and their Senior Leadership Team member (or designee).

5.1.2.2 If the manager/director does not have the authority to determine and declare a non-cybersecurity Major Incident, they report any potential non-cybersecurity Major Incident to their Senior Leadership Team member (or designee).

5.1.3 The Senior Leadership Team member (or their designee) determines if it is a Major Incident (non-cybersecurity) or engages the Chief Information Security Officer for the determination (cybersecurity).

5.1.3.1 If a Major Incident is declared, the person making the determination designates the Incident Response Team Leader and initiates Major Incident Response.

5.1.3.2 If not, they inform the initial reporter, and routine response or remediation is undertaken, consistent with standard operating procedures.

5.1.4 The Chief Information Security Officer (for cybersecurity incidents), or Senior Leadership Team member (non-cybersecurity incidents) informs the CIO of any Major Incident they believe may have reached Disaster level.

5.1.5 If the CIO determines the Major Incident has indeed reached a Disaster level, Disaster Recovery response is initiated in accordance with pertinent OIT Business Continuity/Disaster Recovery Plans.

5.1.6 The Chief Information Security Officer has the authority to declare a Major Incident, and initiate the Major Incident response for any cybersecurity incident.

5.2 Response

5.2.1 The Incident Response Team Leader forms the Incident Response Team and identifies the Communications Coordinator. The Incident Response Team Leader determines whether to activate the *OIT Emergency Operations Center* to help facilitate remediation.

5.2.2 The Incident Response Team Leader consults with the Incident Response Team to confirm the remediation strategy, including Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

5.2.3 The Incident Response Team initiates remediation steps, including any required coordination with other OIT resources, vendors, suppliers, partners, etc.

5.2.4 The Communications Coordinator communicates with AMs and other OIT personnel, as required, to facilitate information flow and official message content.

5.2.5 The Communications Coordinator updates OIT Customer Support. OIT Customer Support posts updates to the CSS page. This is minimally once per hour until remediation. Updating the CSS page automatically updates the OIT Core Status and News (CSN) page. The current Duty Manager is also listed on the CSN Page. To the extent known, the update covers:

5.2.5.1 The nature of the Incident in plain language,

5.2.5.2 The projected impact on agency operations and/or citizens,
5.2.5.3 Quantitative metric(s) of what constitutes remediation,
5.2.5.4 The remediation steps being undertaken,
5.2.5.5 Estimated time for remediation, and *5.2.5.6*
Estimated next update time.

5.2.6 To update the CSN Page, the Communications Coordinator e-mails OIT. CustomerSupport with the Subject line of "Status Page Update". The body of the message should cover the six items identified above. The Communications Coordinator then
calls OIT Customer Support (624-7700) to alert them that this message is waiting.

5.2.7 The AMs, in coordination with the Communications Coordinator ensures that affected agencies are continuously informed.

5.2.8 The CIO communicates with the affected Commissioners.

5.3 Diagnosis & Remediation:

5.3.1 The Incident Response Team diagnoses the cause and estimates remediation time.

5.3.2 The Incident Response Team continuously updates the Communications Coordinator.

5.3.3 The Incident Response Team Leader ensures that a service ticket is created for the Major Incident.

5.3.4 The Incident Response Team performs required remediation. All changes must follow pre-established *emergency change control protocols*[1].

5.3.5 The Incident Response Team Leader determines if/when RTO and RPO are met.

5.4 Post-Remediation:

5.4.1 The Incident Response Team documents the service ticket(s), ensures service tickets are created for any follow-up activities, and that all service tickets are linked.

5.4.2 Upon resolution, the Incident Response Team Leader creates a preliminary report (approved by the CIO prior to distribution), which is distributed to impacted customers (by the AMs) within two business days.

5.4.3 The Incident Response Team Leader creates an OIT Major Incident Report (approved by the CIO prior to distribution), which is distributed to all concerned parties (by the AMs) within five business days of resolution. The report includes full details of the incident and root cause analysis. The report is also attached to the service ticket(s).

6.0 Document Information

[1] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/change-management-policy.pdf

Initial Issue Date: February 26, 2014
Latest Revision Date: May 7, 2019 – to update Document Information.

Point of Contact: Enterprise.Architect@Maine.Gov
Approved By: Chief Information Officer, OIT

Legal Citation: Title 5, Chapter 163: Office of Information Technology[1]. Waiver Process: See the Waiver Policy[2].

[1] http://legislature.maine.gov/statutes/5/title5ch163sec0.html
[2] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf